3GPP TSG-SA WG3 Meeting #36
SHENZHEN, 23-26 November 2004

Tdoc ⌘S3-040921

CR-Form-v7.1

PSEUDO-CHANGE REQUEST

⌘ **33.878** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **0.0.3** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: | UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	A correction about context relationship
Source:	⌘	CCSA/ZTE Corporation
Work item code:	⌘	Early IMS
Date:	⌘	26/10/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	The clause numers in the first sentence of clause 6.3 are wrong.
Summary of change:	⌘	Replace “6.2” with “6.1” in clause 6.3. Replace “6.3” with “6.2” in clause 6.3.
Consequences if not approved:	⌘	The mistake may bring troubles to readers. Need change.

Clauses affected:	⌘	6.3

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	O&M Specifications

⌘

Other comments: ⌘

***** BEGIN SET OF CHANGES *****

6 Threat scenarios

To understand what controls are needed to address the security requirements, it is useful to describe some of the threat scenarios.

NOTE: There are many other threats, which are outside the scope of this TR.

6.1 Impersonation on IMS level using the identity of an innocent user

The scenario proceeds as follows:

- Attacker A attaches to GPRS, GGSN allocates IP address, IP_A
- Attacker A registers in the IMS using his IMS identity, ID_A
- Attacker A sends SIP invite using his own source IP address (IP_A) but with the IMS identity of B (ID_B).

If the binding between the IP address on the bearer level, and the public and private user identities is not checked then the attacker will succeed, i.e. A pays for IP connectivity but IMS service is fraudulently charged to B. The fraud situation is made worse if IP flow based charging is used to 'zero rate' the IP connectivity.

The major problem is however that without this binding multiple users within a group "of friends" could sequentially (or possibly simultaneously) share B's private/public user identities, and thus all get (say) the push-to-talk service by just one of the group paying a monthly subscription. Without protection against this attack, operators could be restricted to IP connectivity based tariffs and, in particular, would be unable to offer bundled tariffs. This is unlikely to provide sufficiently flexibility in today's market place.

6.2 IP spoofing

The scenario proceeds as follows:

- User B attaches to GPRS, GGSN allocates IP address, IP_B
- User B registers in the IMS using his IMS identity, ID_B
- Attacker A sends SIP messages using his own IMS identity (ID_A) but with the source IP address of B (IP_B)

If the binding between the IP address that the GGSN allocated the UE in the PDP context activation and the source IP address in subsequent packets is not checked then the attacker will succeed, i.e. A pays for IMS service but IP connectivity is fraudulently charged to B. Note that this attack only makes sense for IMS services with outgoing traffic only because the attacker will not receive any incoming packets addressed to the IMS identity that he is impersonating.

6.3 Combined threat scenario

The scenario proceeds as follows:

- User B attaches to GPRS, GGSN allocates IP address, IP_B
- User B registers in the IMS using his IMS identity, ID_B
- Attacker A sends SIP messages using IMS identity (ID_B) and source IP address (IP_B)

If the bindings mentioned in the scenarios in clause ~~6.2~~6.1 and ~~6.3~~6.2 are not checked then the attacker will succeed, i.e. A fraudulently charges both IP connectivity and the IMS service to B. Note this attack only makes sense for IMS

services with outgoing traffic only because the attacker will not receive any incoming packets addressed to the IMS identity that he is impersonating.

***** END SET OF CHANGES *****